MWG:KPO/VC
F. #2024R00057

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF (1) A CELLULAR TELEPHONE ASSIGNED PHONE NUMBER 347-499-1498 THAT IS EXPECTED TO BE IN THE POSSESSION OF WINSTON GILLON, AND (2) A CELLULAR TELEPHONE ASSIGNED PHONE NUMBER 347-755-8140, THAT IS EXPECTED TO BE IN THE POSSESSION OF PRESTINA MCLEOD	**TO BE FILED UNDER SEAL** APPLICATION FOR SEARCH WARRANTS FOR ELECTRONIC DEVICES Case No. 24 MC 2823

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR WARRANTS TO SEARCH AND SEIZE

I, ERIN NOLAN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search (a) a cellular telephone assigned phone number 347-499-1498, which is expected to be in the possession of WINSTON GILLON ("GILLON"), as described in Attachment A-1 ("TARGET PHONE 1"); and (b) a cellular telephone assigned phone number 347-755-8140, which is expected to be in the possession of PRESTINA MCLEOD ("MCLEOD"), as described in Attachment A-2 ("TARGET PHONE 2," and together with TARGET PHONE 1, "TARGET PHONES"); for the things described in Attachment B.

2. I am a Special Agent with the United States Postal Service Office of the Inspector General ("USPS-OIG") and have served in this capacity for approximately three years. In this capacity, I am responsible for conducting and assisting investigations into financial fraud

using the United States mails, including investigations into mail theft committed by employees of the United States Postal Service ("USPS"). I have participated in investigations involving, among other things, search warrants and arrest warrants. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

3. This affidavit is based on my personal knowledge, my review of documents and other evidence, conversations with other law enforcement personnel, and my training and experience. This affidavit is intended to show only that there is probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. The United States, including the USPS-OIG and the United States Postal Inspection Service, is investigating the theft of mail, including financial instruments, from the Long Island City Post Office in Long Island City, New York.

5. For the reasons set forth below, I submit that there is probable cause to believe that violations of 18 U.S.C. §§ 371 (Conspiracy to Commit Mail Theft and Commit Theft of Government Funds), 500 (Passing of Forged Money Orders), 641 (Theft of Government Funds), 1702 (Theft of Mail by Postal Service Employee), 1708 (Theft of Mail), and 1028A (Aggravated Identity Theft) (collectively, the "SUBJECT OFFENSES") have been committed by GILLON, MCLEOD, DIANA COAXUM ("COAXUM"), and others known and unknown.

I. Overview of the Scheme

6. GILLON and MCLEOD are both employees of the USPS at the Long Island City Post Office. GILLON works as a mail carrier, and MCLEOD works as a sales and

service/distribution associate, otherwise known as a mail clerk. The two entered into a conspiracy with COAXUM, a fellow USPS employee, and potentially others, to steal over $250,000 in checks issued by the United States Department of the Treasury ("Treasury Checks") starting at least as early as November 2021 and continuing until November 2022. COAXUM and MCLEOD also stole and fraudulently cashed money orders issued by the USPS, known as "Postal Money Orders," or "PMOs."

7. GILLON, MCLEOD and COAXUM used their access as USPS employees to steal Treasury Checks and PMOs from the mail, and then MCLEOD or COAXUM would cash the checks in their capacity as clerks. In doing so, MCLEOD and COAXUM would either write fake identifying information on the reverse of the check or use real identifying information for a USPS customer who was not the payee. In all cases, they had no authorization from the rightful payees to cash these checks.

8. In addition to personally cashing stolen checks at the Long Island City Post Office, the conspiracy also involvement transferring stolen checks to other individuals. For instance, the investigation revealed that in collaboration with COAXUM, GILLON stole two Treasury Checks—totaling nearly $60,000—and transferred them to another individual who deposited them into his account in August 2022 by altering the payee's name and address.[1]

9. On July 8, 2024, a grand jury sitting in the Eastern District of New York returned a sealed indictment (the "Indictment," attached as Exhibit 1) charging GILLON and MCLEOD with violations of 18 U.S.C. §§ 371 (Conspiracy to Commit Mail Theft and Commit Theft of Government Funds), 1702 (Theft of Mail by Postal Service Employee), and 641 (Theft

[1] These checks are not included in the $250,000 estimate which refers only to those checks fraudulently and personally cashed by MCLEOD and GILLON.

of Government Funds). The Indictment also charges MCLEOD only with violations of 18 U.S.C. § 1028A (Aggravated Identity Theft). See 24-CR-274 (sealed). The Indictment remains sealed, and neither GILLON nor MCLEOD have been arrested.

10. COAXUM was charged separately in 2022 in the Eastern District of New York, and she ultimately pleaded guilty to a violation of 18 U.S.C. § 641 (Theft of Government Funds). COAXUM is awaiting sentencing. See United States v. Coaxum, No. 22-CR-522 (E.D.N.Y.).

II. Use of the TARGET PHONES in Committing the SUBJECT OFFENSES

11. COAXUM's cellular telephone was seized incident to her arrest, and a search warrant was obtained (No. 22-MJ-1268). COAXUM's cellular telephone showed the coordination by text message between COAXUM and GILLON (using TARGET PHONE 1), and between COAXUM and MCLEOD (using TARGET PHONE 2). Some examples are provided below.

A. Theft of a U.S. Treasury Check by MCLEOD and COAXUM

12. On August 23, 2022, at 4:47 p.m., COAXUM cashed a U.S. Treasury check in the amount of $1,137.54 at the Long Island City Post Office. The check number ended in 9648 and was made payable to "Jonathan H Stevenson and Sharon L But."

13. Surveillance footage from the Long Island City Post Office shows the theft. Specifically, COAXUM can be seen removing from her desk a small sheet of paper, consistent with the size of a Treasury check, at 4:43 p.m. while a customer was at her window, but continuing to process a transaction after that customer left. At the same time that she appeared on the surveillance video to finish processing the transaction at her desk, the above-described U.S. Treasury check in the amount of $1,137.54 was cashed. Later that day, when

COAXUM returned her cash drawer to the safe, she can be seen on surveillance video footage stuffing cash into her shirt.

14. Earlier that day, MCLEOD (using TARGET PHONE 2) and COAXUM exchanged text messages concerning the theft of this Treasury check:

> MCLEOD (1:23 p.m.): I got one
>
> COAXUM (1:23 p.m.): Wordddd
>
> COAXUM (1:23 p.m.): Finally! We been having a dry spell
>
> COAXUM (1:23 p.m.): Yo Amex can get us gas so keep that in mind
>
> MCLEOD (1:24 p.m.): Nobody Lml where u parked it's 1000 that if u make it we could do it today
>
> MCLEOD (1:24 p.m.): Ok
>
> COAXUM (1:24 p.m.): Imma try to as soon as I get back
>
> COAXUM (1:24 p.m.): Sign it

Based on my training, experience, and investigation of this case to date, I have probable cause to believe that these messages concerned MCLEOD's theft of the above-described Treasury check in the amount of $1,137.54 ("I got one"), which she described as being worth $1,000 ("it's 1000"). I further believe that, in these messages, MCLEOD was asking COAXUM to process the stolen check later that day ("if u make it we could do it today").

15. This U.S. Treasury check was reported stolen, and one of the intended payees later reported to law enforcement that he had not received the check or cashed it, and that and he was not aware of anyone else having cashed it.

B. Theft of Another U.S. Treasury Check by MCLEOD and COAXUM

16. Postal records reveal that on Saturday, October 22, 2022, MCLEOD processed a U.S. Treasury check in the amount of $1,477.85, which was made payable to "D.P. Facilities Inc[.]"

17. Text messages between MCLEOD (using TARGET PHONE 2) and COAXUM reveal their coordination in the theft of this check:

> MCLEOD (October 14, 2022, 4:49 p.m.): U got 14
>
> COAXUM (October 14, 2022, 4:50 p.m.): Save that for Monday
>
> MCLEOD (October 14, 2022, 4:51 p.m.): Ok
>
> COAXUM (October 20, 2022, 12:58 p.m.): Yooo did u take care if the 14
>
> COAXUM (October 20, 2022, 12:58 p.m.): Of**
>
> MCLEOD (October 20, 2022, 12:58 p.m.): No
>
> COAXUM (October 21, 2022, 3:27 p.m.): Sign the whole name
>
> MCLEOD (October 21, 2022, 3:27 p.m.): Ok
>
> MCLEOD (October 21, 2022, 4:53 p.m.): U got it?
>
> COAXUM (October 25, 2022, 12:53 p.m.): Bring it to me
>
> MCLEOD (October 25, 2022, 12:54 p.m.): I did that one Saturday ima try to get some today cuz it's looking crazy

Based on my training, experience, and investigation of this case to date, I believe that these messages concerned the conspiracy to steal U.S. Treasury checks. First, the amount of the check ($1,477.85) matches MCLEOD's initial request of whether COAXUM had "14" (i.e., $1400) in cash in her drawer to cash, and COAXUM's query as to whether MCLEOD had taken care of "the 14." Second, MCLEOD responded on October 25 that she "did that one Saturday," and this U.S. Treasury check was, in fact, cashed on October 22, the most recent Saturday.

18. Other evidence is consistent with MCLEOD's theft of the check and its proceeds. A consent search of MCLEOD's locker was conducted on November 21, 2022, and a receipt for cashing this check in the amount of $1,477.85 was found in her locker.

C. Theft of a Money Order by MCLEOD and COAXUM

19. Text messages between MCLEOD (using TARGET PHONE 2) and COAXUM on November 8, 2022 show their coordination to steal a PMO later that same day:

COAXUM (3:01 p.m.): I have a MO if u wanna do it

COAXUM (3:01 p.m.): It's 800

MCLEOD (3:04 p.m.): Yea

COAXUM (3:06 p.m.): Ok when I go on break imma get it

MCLEOD (3:06 p.m.): Ok sign it n fill it out so I cud just do it real quick

COAXUM (3:06 p.m.): Ok

MCLEOD (4:40 p.m.): They gotta go

COAXUM (4:40 p.m.): If you do it now they not pay attention

Based on my training, experience, and investigation of this case to date, I believe that these messages concern the theft of a PMO because of the reference to "MO," meaning "money order," and the direction to "fill it out [. . .] real quick" based on the process for cashing PMOs in post offices.

20. Only two minutes after that last text message from COAXUM, MCLEOD processed a PMO in the amount of $800, which was made payable to "GVS Properties LLC." The payor reported the PMO as wrongfully paid to another person.

D. GILLON and COAXUM's Efforts to Identify High-Value Checks

21. On August 4, 2022, COAXUM texted GILLON (using TARGET PHONE 1), "Nothing small[,] right[?]" to which GILLON replied, "Nah nothing small." COAXUM then asked, "No 4k[?]" to which he responded, "I will check." COAXUM then texted: "He said the reason why he wanted them is so he can start working on them cuz we have to create stuff for them and that takes time and the longer we hold the higher the chances are that it will clip the account[.] So if you want u can pass me the 111 and another high one[.]"

22. Based on my training, experience, and investigation of this case to date, I have probable cause to believe that these messages indicate that: (a) GILLON was searching for checks to provide to COAXUM, (b) they were receiving direction from another individual, (c) and GILLON was holding for COAXUM a check for "111" (presumably $111,000) and "another high one [i.e., check]."

E. GILLON Admits to the Theft of a $35,576.73 Check

23. On August 10, 2022, GILLON (using TARGET PHONE 1) sent a text to COAXUM: "I think this is the one for 35. I didn't think you gave that one to him but I guess you did." Along with this message, GILLON sent COAXUM an image of a U.S. Treasury Check in the amount of $35,567.73—one of the two stolen Treasury Checks totaling nearly $60,000 described above.

F. GILLON Provides COAXUM with a $7,585.01 Treasury Check

24. On August 25, 2022, COAXUM texted GILLON (using TARGET PHONE 1) asking for something "small . . . [l]ike for 2000 or 3000." GILLON replied that he had "a business for 7500," to which COAXUM responded, "I need to try to get that done." In

response to another message five days later, GILLON texted COAXUM: "[T]he one I told you about. 7500."

25. Nine days later, on or about September 8, 2022, Coaxum used an invalid ID number to cash a $7,585.01 check made payable to a business whose address is on GILLON's route.

III. The TARGET PHONES

26. TARGET PHONE 1 has been attributed to GILLON based on the following evidence:

a. According to information obtained from TARGET PHONE 1's carrier, GILLON's wife is the listed subscriber of TARGET PHONE 1.

b. TARGET PHONE 1 is saved in COAXUM's phone as "Winstin," and GILLON's first name is "Winston."

c. USPS employee records list TARGET PHONE 1 as GILLION's contact phone number.

27. TARGET PHONE 2 has been attributed to MCLEOD based on the following evidence:

a. According to information obtained from TARGET PHONE 2's carrier, MCLEOD is the listed subscriber of TARGET PHONE 2.

b. TARGET PHONE 2 is saved in COAXUM's phone as "Prestina," which is MCLEOD's first name.

c. USPS employee records list TARGET PHONE 2 as MCLEOD's contact phone number.

* * *

28. I respectfully submit that the information above establishes probable cause to believe that the TARGET PHONES contains evidence of the SUBJECT OFFENSES. Among other things, the evidence shows that GILLON and MCLEOD used their cellular devices to coordinate and execute their commission of the SUBJECT OFFENSES.

IV. The Requested Searches

29. Law enforcement agents plan to arrest both GILLON and MCLEOD at locations within the Eastern District of New York within 14 days of the issuance of the applied-for warrants.

30. To execute the search of TARGET PHONE 1, law enforcement officers will locate any cellular devices that are in the possession, custody, or control of GILLON, including on GILLON's person or those stored in closed bags that are in his possession, custody, or control when law enforcement agents arrest GILLON in the Eastern District of New York. Agents will then ascertain whether any of those cellular devices are assigned call number 347-499-1498. If so, law enforcement agents will seize TARGET PHONE 1 and will then conduct the forensic examination of TARGET PHONE 1 for the purpose of identifying electronically stored data particularly described in Attachment B.

31. Similarly, to execute the search of TARGET PHONE 2, law enforcement officers will locate any cellular devices that are in the possession, custody, or control of MCLEOD, including on MCLEOD's person or those stored in closed bags that are in her possession, custody, or control when law enforcement agents arrest MCLEOD in the Eastern District of New York. Agents will then ascertain whether any of those cellular devices are assigned call number 347-755-8140. If so, law enforcement agents will seize TARGET PHONE

2 and will then conduct the forensic examination of TARGET PHONE 2 for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

32. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a

variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each

satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an

IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

33. Based on my training, experience and research, I know that the TARGET PHONES have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices and PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the TARGET PHONE.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

34. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

35. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant, but also for forensic evidence that establishes

how the TARGET PHONES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET PHONES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

36. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

37. Biometric unlocking. The applied-for warrants also would permit law enforcement to obtain from MCLEOD and GILLON the display of physical biometric characteristics (such as fingerprint, thumbprint or facial characteristics) to unlock the TARGET PHONES.

38. Based on my training and experience, I know that many electronic devices offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. If the device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through the camera recognizing his or her face. Some devices offer a combination of these features and the user of such devices can select which features they would like to use.

39. Based on my training and experience, I know that users of electronic devices often enable the biometric features because they are considered to be more convenient

ways to unlock a device than by entering the passcode or password. In some instances, biometric features are also considered to be a more secure way to protect the devices' contents. This is particularly true when the users of a device are engaged in criminal activity and thus have a heightened concern about securing the contents of the device.

REQUEST FOR SEALING

40. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. MCLEOD and GILLON do not have knowledge of this investigation, and they remain at liberty. If they were to become aware this investigation, they may flee to avoid prosecution and destroy evidence, much of which is stored in an electronic format. Therefore, premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

CONCLUSION

41. I submit that this affidavit supports probable cause for search warrants authorizing the examination of the TARGET PHONES described in Attachments A-1 and A-2 to seek the items described in Attachment B.

Respectfully submitted,
/s/ Erin Nolan
Erin Nolan
Special Agent
United States Postal Service – Office of the Inspector General

Subscribed and sworn to before me by telephone on July 18, 2024

Lois Bloom
HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A-1

The property to be seized and searched is a cellular telephone assigned phone number 347-499-1498 ("TARGET PHONE 1") that is expected to be in the possession, custody, or control of WINSTON GILLON ("GILLON") when law enforcement agents encounter GILLON at a location within the Eastern District of New York. The property to be searched includes GILLON's person and any closed bags in his possession, custody, or control which may contain TARGET PHONE 1 when law enforcement agents encounter GILLON at a location within the Eastern District of New York.

This warrant authorizes the forensic examination of TARGET PHONE 1 for the purpose of identifying the electronically stored information described in Attachment B.

Law enforcement personnel are authorized to seize TARGET PHONE 1 from GILLON's person or clothing, personal items, and containers (e.g., backpacks, wallets, briefcases, and bags) in his physical possession, and, during the execution of this search warrant, are authorized to depress the fingerprints and/or thumbprints of GILLON onto the Touch ID sensor of TARGET PHONE 1, or hold TARGET PHONE 1 in front of GILLON's face and/or eyelids in order to gain access to the contents of TARGET PHONE 1 as authorized by this warrant. However, law enforcement personnel are not authorized to hold open GILLON's eyelids to enable law enforcement to unlock TARGET PHONE 1.

While attempting to unlock TARGET PHONE 1 by the use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement personnel are not authorized to demand that GILLON state or otherwise provide the password or identify the specific biometric characteristics (such as the unique finger(s) or other physical features) that may be used to unlock TARGET PHONE 1. However, voluntary disclosure of such information by

GILLON is permitted. To avoid confusion on this point, if law enforcement is executing the warrant and asks GILLON or any other persons for the passwords to TARGET PHONE 1, or to identify which biometric characteristics (such as the unique finger(s) or other physical features) unlocks TARGET PHONE 1, law enforcement will not state or otherwise imply that the warrant requires the person to provide such information. Law enforcement will make clear that providing any such information is voluntary and that the person is free to refuse the request.

ATTACHMENT A-2

The property to be seized and searched is a cellular telephone assigned phone number 347-755-8140 ("TARGET PHONE 2") that is expected to be in the possession, custody, or control of PRESTINA MCLEOD ("MCLEOD") when law enforcement agents encounter MCLEOD at a location within the Eastern District of New York. The property to be searched includes MCLEOD's person and any closed bags in her possession, custody, or control which may contain TARGET PHONE 2 when law enforcement agents encounter MCLEOD at a location within the Eastern District of New York.

This warrant authorizes the forensic examination of TARGET PHONE 2 for the purpose of identifying the electronically stored information described in Attachment B.

Law enforcement personnel are authorized to seize TARGET PHONE 2 from MCLEOD's person or clothing, personal items, and containers (e.g., backpacks, wallets, briefcases, and bags) in his physical possession, and, during the execution of this search warrant, are authorized to depress the fingerprints and/or thumbprints of MCLEOD onto the Touch ID sensor of TARGET PHONE 2, or hold TARGET PHONE 2 in front of MCLEOD's face and/or eyelids in order to gain access to the contents of TARGET PHONE 2 as authorized by this warrant. However, law enforcement personnel are not authorized to hold open MCLEOD's eyelids to enable law enforcement to unlock TARGET PHONE 2.

While attempting to unlock TARGET PHONE 2 by the use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement personnel are not authorized to demand that MCLEOD state or otherwise provide the password or identify the specific biometric characteristics (such as the unique finger(s) or other physical features) that may be used to unlock TARGET PHONE 2. However, voluntary disclosure of such information

by MCLEOD is permitted. To avoid confusion on this point, if law enforcement is executing the warrant and asks MCLEOD or any other persons for the passwords to TARGET PHONE 2, or to identify which biometric characteristics (such as the unique finger(s) or other physical features) unlocks TARGET PHONE 2, law enforcement will not state or otherwise imply that the warrant requires the person to provide such information. Law enforcement will make clear that providing any such information is voluntary and that the person is free to refuse the request.

ATTACHMENT B

1. All information or records on TARGET PHONE 1 and TARGET PHONE 2 (collectively, the "TARGET PHONES") described in Attachments A-1 and A-2 that relate to violations of Title 18, United States Code, Sections 371 (Conspiracy), 500 (Passing of Forged Money Orders), 641 (Theft of Government Funds), 1702 (Theft of Mail by Postal Service Employee), 1708 (Postal Theft) and 1028A (Aggravated Identity Theft) (the "SUBJECT OFFENSES") by WINSTON GILLON, PRESTINA MCLEOD, and DIANA COAXUM for the period between September 1, 2021 and December 31, 2022.

a. Communications regarding the SUBJECT OFFENSES;

b. Lists of co-conspirators and related identifying information;

c. Notes, documents, records, invoices, bank statements, or correspondence in any format, such as chat logs, electronic messages, and web cache information related to the SUBJECT OFFENSES;

d. Financial transactions and records relating to the SUBJECT OFFENSES;

e. Photographs, videos or other images relating to the SUBJECT OFFENSES; and

f. Evidence of user attribution showing who used or owned the TARGET PHONES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or

stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.